UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JOHN PRIDDY, RANDY MCGILBERRY, TIMOTHY JEMISON, NATHANIEL GERTH, GARY BECKER, AMINE M. BENDRISS, BARBARA BROWN, DAVID PACHOLCZAK, PATRICIA MCMAHON, and EVAN WEESE, on behalf of themselves and others similarly situated,	*	
Plaintiffs,	*	Civil Action No. 1:23-cv-10575-IT
v.	*	
ZOLL MEDICAL CORPORATION,	*	
Defendant.	*	

MEMORANDUM & ORDER

March 31, 2025

TALWANI, D.J.

In this consolidated putative class action data-breach dispute relating to a data breach that purportedly compromised the private information of over a million people, ten Plaintiffs bring state common law claims against Defendant ZOLL Medical Corporation ("ZOLL Medical") for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and declaratory judgment and injunctive relief. Plaintiffs also bring state statutory claims as follows: Plaintiffs Randy McGilberry and Barbara Brown (the "Florida Plaintiffs") claim violations of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201; Plaintiff Gary Becker, a Kansas resident, claims violations of the Kansas Consumer Protection Act ("KCPA"), Kan. Stat. Ann. §§ 50-623; Plaintiff David Pacholczak, a New York resident, claims violations of the New York General Business Law ("NY GBL"), N.Y. Gen. Bus.

Law §§ 349, et seq.; Plaintiff Amine Bendriss, a Pennsylvania resident, claims violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 P.S. § 201-3; and Plaintiffs John Priddy and Patricia McMahon (the "Illinois Plaintiffs") claim violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 ILCS 505/1.[1] Plaintiffs seek to certify a nationwide class of all persons residing in the United States whose private information was impacted by the data breach, subclasses for customers in Florida, Kansas, New York, Pennsylvania, and Illinois whose private information was impacted by the data breach, and subclasses for current and former employees whose private information was impacted by the data breach.

Pending before the court is ZOLL Medical's Motion to Dismiss [Doc. No. 36] Plaintiffs' Consolidated Class Action Complaint ("Complaint") [Doc. No. 33] for lack of standing under Federal Rule of Civil Procedure ("FRCP") 12(b)(1) and for failure to state a claim under FRCP 12(b)(6). For the reasons set forth below, ZOLL Medical's motion is granted in part and denied in part.

I. Plaintiffs' Allegations

The Complaint alleges as follows:

ZOLL Medical produces a variety of advanced emergency care devices, including ones that provide defibrillation and cardiac monitoring, circulation enhancement and CPR feedback, supersaturated oxygen therapy, and ventilation. Compl. ¶ 2 [Doc. No. 33]. Plaintiffs are current

[1] Plaintiffs Timothy Jemison, Nathaniel Gerth, and Evan Weese have not asserted any statutory claims. Robert Smith, who filed the first proceeding in this consolidated action, has not asserted a claim in the Consolidated Class Action Complaint [Doc. No. 33], see id. at 1 n.1, and has been removed from the caption.

and former patients[2] and/or employees[3] of ZOLL Medical, from whom ZOLL Medical collected personally identifying information ("PII") and protected health information ("PHI") (collectively, "Private Information"). Id. ¶¶ 2-3, 34, 90. This Private Information was then stored on ZOLL Medical's computer network. Id. ¶ 34. In its online privacy policy, ZOLL Medical represented that it "[had] implemented measures designed to secure [Plaintiffs' and Putative Class Members'] personal information from accidental loss and unauthorized access, use, alteration, and disclosure." Id. ¶ 40.

Plaintiffs took reasonable precautions when sharing and securing their sensitive PII by not knowingly transmitting such information unencrypted over the internet, storing documents with such information in secure locations or destroying them, and diligently using unique usernames and passwords; Plaintiffs also took reasonable precautions as to their Private Information by using multifactor authentication when available. Id. ¶¶ 99, 112, 127, 142, 157, 172, 186, 201, 216, 230. Plaintiffs only allowed ZOLL Medical to maintain, store, and use their Private Information because they believed that ZOLL Medical would use basic security measures to protect it. Id. ¶¶ 100, 113, 128, 143, 158, 173, 187, 202, 217, 231.

On January 28, 2023, ZOLL Medical detected unusual activity on its internal computer network and later confirmed that Plaintiffs' Private Information had been impacted in a data breach (the "Data Breach"). Id. ¶ 42. In March 2023, ZOLL Medical began issuing notice letters to Plaintiffs to notify them of this Data Breach. Id. ¶ 92. The sample Notice Letter attached to the

---

[2] Plaintiffs Priddy, McGilberry, Jemison, Becker, Bendriss, Brown, Pacholczak, and McMahon are former patients. Id. ¶¶ 96, 109, 124, 154, 169, 183, 198, 213.

[3] Plaintiffs Gerth and Weese are former employees. Id. ¶¶ 139, 227.

Complaint states that "[i]nformation that may have been disclosed includes your name, address, date of birth, and Social Security numbers." Id. ¶ 43 & Ex. 1.[4] The Notice Letters stated further that "[i]t may also be inferred that you used or were considered for use of a ZOLL product." Id. Following the breach, ZOLL Medical offered identity-monitoring services to Plaintiffs for a period of 24 months. Id. ¶ 53. ZOLL Medical has not informed Plaintiffs what data was stolen, the method of disclosure, the results of any investigations, or any steps it has taken to secure Plaintiffs' Private Information going forward. Id. ¶ 54.

Because of the Data Breach, Plaintiffs' Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and placed for sale on the dark web. Id. ¶¶ 102, 115, 130, 145, 160, 175, 189, 204, 219, 233. Seven of the ten named plaintiffs—Randy McGilberry, Timothy Jemison, Nathaniel Gerth, Gary Becker, Barbara Brown, David Pacholczak, and Evan Weese—suffered from incidents of misuse of their Private Information after the Data Breach, including successful or attempted fraudulent transactions on their debit and credit cards, id. ¶¶ 116, 131, 146, 161, 190, 205, 234; unauthorized applications for credit cards in their names, id. ¶ 131; medical bills or charges issued from unknown sources, id. ¶¶ 131;[5] and notifications that their Private Information had been found on the dark web, id.

---

[4] The Complaint does not allege that each Plaintiff received this exact letter, and alleges only as to Plaintiffs McMahon and Weese that the notice letters specifically notified them that their Social Security numbers had been potentially compromised. Id. ¶¶ 214-15, 228-29.

[5] Plaintiff McMahon "received notice of an inaccurate charge to her Medicare account for a catheter, a device which she does not have and has never been prescribed." Id. ¶ 220. It is unclear if this was a fraudulent rather than merely mistaken charge, but because Plaintiffs omit this allegation from their brief's recitation of "actual misuse of [seven Plaintiffs'] Private Information," see Pls.' Opp. to Def.'s Mot. to Dismiss ("Opp.") at 6-7 [Doc. No. 38], the court does not draw the inference that McMahon's Private Information was actually misused.

¶ 234. Additionally, nine of the ten named Plaintiffs reported a "dramatic increase" in spam and phishing attempts targeted at them, including attempts advertising medical devices. Id. ¶¶ 103, 117, 132, 147, 162, 176, 191, 206, 220. All named Plaintiffs have spent "significant time" verifying the legitimacy of their Notice Letters and continually self-monitoring their accounts and credit reports to check for fraudulent activity. Id. ¶¶ 106, 120, 135, 150, 165, 179, 194, 209, 223, 237. The quantification of this time ranges from an hour a week to 60 hours at the time of the Complaint. See, e.g., id. ¶¶ 105, 136, 149, 164.

In December 2023, ZOLL Medical disclosed another cybersecurity incident that compromised the PHI, names, addresses, Social Security numbers, and insurance information of current and former ZOLL Medical employees as well as those of their dependents and beneficiaries. Id. ¶¶ 358-59. ZOLL Medical characterized this incident as an email phishing attack targeted at a ZOLL Medical employee. Id. ¶ 359.

II. Standing

ZOLL Medical argues that Plaintiffs lack standing for several reasons: (1) the alleged financial fraud is not traceable to ZOLL Medical because no credit or debit card data was impacted in the Data Breach; (2) injury-in-fact cannot be established upon mere exposure of Plaintiffs' Private Information, increased receipt of spam, overpayment where no benefit of the bargain was lost, diminution in the value of Private Information, or anxiety and annoyance; (3) injunctive relief would not redress any future injury because Plaintiffs allege that their Private Information has already been accessed. Def.'s Mem. ISO Mot. to Dismiss ("Def.'s Mem.") at 8-14 [Doc. No. 37].

This court finds that Plaintiffs have standing because they have plausibly alleged that some Private Information impacted by the Data Breach has already been misused in incidents of financial fraud fairly traceable to ZOLL Medical. They have also alleged a material risk of their Private Information being misused in the future, which is redressable by injunctive relief. Plaintiffs also have standing for their alleged injuries of emotional distress and lost benefit of the bargain. However, Plaintiffs do not have standing based on the alleged injuries of increased spam or diminution in value of their Private Information.

A. Standard of Review

The doctrine of standing derives from Article III of the Constitution, which confines federal courts to the adjudication of actual "cases" and "controversies." See U.S. Const. art. III, § 2, cl. 1; Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992). To establish standing, "[t]he plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016) (quoting Lujan, 504 U.S. at 560–61). Where no class is yet certified, the court "evaluate[s] only whether the [named] plaintiff[s have] constitutional [ ] standing to pursue the action." Katz v. Pershing, LLC, 672 F.3d 64, 71 (1st Cir. 2012).

As to injury-in-fact, certain harms "readily qualify as concrete injuries," most obviously the traditional tangible harms: physical and monetary. TransUnion LLC v. Ramirez, 594 U.S. 413, 425 (2021) (citation omitted). Intangible harms can be concrete when they enjoy "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts," such as "reputational harms, disclosure of private information, and intrusion upon

seclusion." Id. "'[A] material risk of future harm can [also] satisfy the concrete-harm requirement,' but only as to injunctive relief, not damages." Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 372 (1st Cir. 2023) (quoting TransUnion, 594 U.S. at 435). For standing to pursue damages, a plaintiff must demonstrate a separate concrete harm caused "by their exposure to the risk itself." Id. (quoting TransUnion, 594 U.S. at 437).

As to redressability, "plaintiffs need not quantify or offer a formula for quantifying their injury." In re Evenflo Co., Inc., Mktg., Sales Pracs. & Prod. Liab. Litig., 54 F.4th 28, 40 (1st Cir. 2022). With respect to claims for damages, so long as monetary relief would compensate a plaintiff for his injury, such injury is redressable. Id. at 41. Injunctive relief, however, depends on whether plaintiffs are "likely to suffer future injury." Webb, 72 F.4th at 378 (citation omitted).

Because standing is not a "mere pleading requirement[] but rather an indispensable part of the plaintiff's case," standing must be supported "with the manner and degree of evidence required at the successive stages of the litigation." Lujan, 504 U.S. at 561; see also TransUnion LLC, 594 U.S. at 431. At the pleading stage, "the plaintiff must 'clearly . . . allege facts demonstrating' each element" of standing. Spokeo, 578 U.S. at 338 (quoting Warth v. Seldin, 422 U.S. 490, 518 (1975)). The court applies "'the same plausibility standard used to evaluate a motion under Rule 12(b)(6).'" Webb, 72 F.4th at 371 (quoting Gustavsen v. Alcon Lab'ys, Inc., 903 F.3d 1, 7 (1st Cir. 2018)).

B. Injury-in-Fact and Traceability[6]

1. Actual Misuse of the Private Information

The alleged financial fraud experienced by Plaintiffs McGilberry, Jemison, Gerth, Becker, Brown, Pacholczak, and Weese supports their standing.[7] The fraud they allege is fairly traceable to ZOLL Medical because of the temporal and logical connection between the fraud and the Data Breach.

This court is guided by the First Circuit's decision in Webb, which found an "obvious temporal connection" between the timing of a data breach and the subsequent filing of a false tax return. 72 F.4th at 374. There, the defendant home-delivery pharmacy service suffered a January 2021 data breach that compromised the PII it had collected from its patients, including the plaintiff. Id. at 369-70. Subsequently, the plaintiff's compromised information was used to file a false 2021 tax return in her name. Id. at 370. This sufficed to draw a plausible connection between the actual misuse of the plaintiff's information and the data breach in which that information had been compromised. Id. at 374. The First Circuit also noted that the plaintiff was "very careful about sharing her PII," had "never knowingly transmitted unencrypted PII over the

---

[6] The parties do not suggest the standing inquiry differs with respect to any particular cause of action. Because the allegations arise from a single data breach and are intertwined across all claims, the court treats the claims together throughout its analysis except where otherwise specified. See Webb, 72 F.4th at 373 n.3.

[7] The court does not adopt ZOLL Medical's narrow characterization of misuse as only including successful debit or credit card fraud while excluding fraudulent medical bills and attempted debit or credit card fraud. See Def.'s Mem. at 5-6, 8-9 [Doc. No. 37]. ZOLL Medical relies on I.C. v. Zynga, Inc., 600 F. Supp. 3d 1034, 1052 (N.D. Cal. 2022), for the proposition that unsuccessful attempts at fraud "cannot plausibly be considered independent injuries." But the court there was addressing "credential stuffing, phishing attacks, and [] various forms of spam," id., not specific allegations of attempted fraudulent transactions.

internet or any other unsecured source," and stored documents containing this information in a secure location. Id. From these allegations, the First Circuit drew the "obvious inference" that those who filed the false tax return obtained the plaintiff's compromised information from the data breach. Id.

Similarly here, Plaintiffs are alleged to be reasonably cautious with securing their Private Information, Compl. ¶¶ 99, 112, 127, 142, 157, 172, 186, 201, 216, 230 [Doc. No. 33], and to have experienced financial fraud after their Private Information was compromised in the Data Breach. Although the Complaint does not identify the date of each incident of financial fraud, the Data Breach occurred on January 28, 2023, and Plaintiffs filed this Complaint on February 26, 2024; thus, at most thirteen months elapsed between the Data Breach and the alleged financial fraud. The Webb court similarly did not identify when the false 2021 tax return was filed, but at most sixteen months had elapsed there. Webb, 72 F.4th at 370; see also In re LastPass Data Sec. Incident Litig., 742 F. Supp. 3d 109, 122 (D. Mass. 2024) (finding "obvious temporal connection" without specifying dates, where plaintiffs "plausibly alleged third parties obtained their sensitive information from the data breach and not from elsewhere" and plaintiffs were "careful" to safeguard that information). Cf. Santos-Pagan v. Bayamon Med. Ctr., 2024 WL 4350990, at *7 (D.P.R. Sept. 30, 2024) (finding no temporal connection where no "specific timeframe" was provided and plaintiff did not attest to carefully safeguarding her information or "aver that setting up the fraudulent cellphone account would have required the same information [defendant] had in her file"). A plausible inference can thus be drawn between the Data Breach and the alleged financial fraud that Plaintiffs suffered.

As to a logical connection, ZOLL Medical contends that no credit or debit card data was impacted in the Data Breach (or ever provided to ZOLL Medical), so any alleged credit and debit card fraud cannot be traced to the Data Breach. Def.'s Mem. at 8 [Doc. No. 37]. However, Plaintiffs plausibly allege that cyber-criminals could have assembled "Fullz" packages by coupling Private Information obtained from the Data Breach with unregulated data available elsewhere to assemble complete dossiers on individual victims. Compl. ¶ 248 [Doc. No. 33]. These packages can be sold and "cashed out" in various ways, such as by performing bank transactions over the telephone using authentication details obtained from the Data Breach. Id. ¶ 247 n.23. Other courts have credited such theories, noting that "[e]ven if the data accessed in the Data Breaches did not provide all the information necessary to inflict these harms, they very well could have been enough to aid therein." In re Mednax Servs., Inc., Customer Data Sec. Breach Litig., 603 F. Supp. 3d 1183, 1203 (S.D. Fla. 2022); see also Fox v. Iowa Health Sys., 399 F. Supp. 3d 780, 792 (W.D. Wis. 2019) ("reasonably infer[ring] that scammers took the health information from the data breaches and cross-referenced it with Fox's contact information from another source" where defendant failed to challenge allegations about "fullz packages"). ZOLL Medical offers no authority to the contrary. For the same reason, the fact that not all Plaintiffs were notified that their Social Security numbers were exposed, see Def.'s Mem. at 5 [Doc. No. 37], does not itself dispose of a logical connection between the Data Breach and the misuse of Private Information here. See In re Zappos.com, Inc., 888 F.3d 1020, 1027 (9th Cir. 2018) (crediting allegation that "the type of information accessed in the [data] breach," which did not include social security numbers, "can be used to commit identity theft, including by . . . exploit[ing] information [hackers] already have to get even more PII").

Moreover, Plaintiffs plausibly allege that ZOLL Medical's "actions led to the exposure and actual or potential misuse of the plaintiffs' PII, making their injuries fairly traceable to [ZOLL Medical's] conduct." Webb, 72 F.4th at 377. Specifically, they allege that ZOLL Medical "could have prevented the Data Breach by properly securing and encrypting . . . Plaintiffs' and Class Members' Private Information," Compl. ¶ 55 [Doc. No. 33], which was instead left "accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals," id. ¶ 44. Furthermore, ZOLL Medical allegedly failed to comply with Federal Trade Commission ("FTC") guidelines identifying best data security practices, id. ¶¶ 71-77; failed to follow industry standards, id. ¶¶ 78-83; and violated other standards including those mandated by the Health Insurance Portability and Accountability Act ("HIPAA"), id. ¶¶ 84-89. Taken as true for purposes of the pending motion, these allegations are sufficient to support Plaintiffs' claim that the financial fraud is fairly traceable to the challenged conduct of ZOLL Medical.

Accordingly, the court finds that Plaintiffs McGilberry, Jemison, Gerth, Becker, Brown, Pacholczak, and Weese have standing to bring claims based on actual misuse of their Private Information allegedly obtained in the Data Breach.

2. Risk of Future Misuse of the Private Information

The court also finds standing for all Plaintiffs based on allegations of a material risk of future misuse of their Private Information.

Plaintiffs allege that the Data Breach caused them to suffer "substantially increased risk" of additional future fraud, identity theft, and misuse of their Private Information. Id. ¶¶ 104, 118, 133, 148, 163, 177, 192, 207, 221, 235. ZOLL Medical contends that the mere exposure of

Plaintiffs' Private Information cannot constitute actual misuse of data and thus cannot constitute injury-in-fact. Def.'s Mem. at 9-11 [Doc. No. 37].

Evaluating the risk of future misuse from a data breach is a fact-specific inquiry, for which the First Circuit has taken guidance from the Second Circuit's non-exhaustive McMorris factors: "(1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." Webb, 72 F.4th at 375 (quoting McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 303 (2d Cir. 2021)). As to the sensitivity of data, "dissemination of high-risk information such as Social Security numbers and dates of birth—especially when accompanied by victims' names—makes it more likely that those victims will be subject to future identity theft or fraud." Id. at 376 (citation omitted). The First Circuit has also held that "the actual misuse of a portion of the stolen information increases the risk that other information will be misused in the future." Id. at 375.

Here, Plaintiffs allege that the Data Breach was the result of a targeted attack on ZOLL Medical. Compl. ¶ 45 [Doc. No. 33]. As discussed above, the alleged financial fraud already experienced by some Plaintiffs is fairly traceable to ZOLL Medical, and Plaintiffs further allege that Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and placed for sale on the dark web. Id. ¶¶ 102, 115, 130, 145, 160, 175, 189, 204, 219, 233.

Finally, Private Information exposed in the Data Breach included names, dates of birth, and at least some Social Security numbers—data so sensitive as to elevate the risk of identity

theft or fraud. Id. ¶¶ 43, 215, 229. ZOLL Medical underscores that only two named Plaintiffs received notice letters indicating their Social Security numbers had been impacted by the Data Breach. Def.'s Mem. at 5-6 [Doc. No. 37]. And the Complaint does not specify which of the other named Plaintiffs, if any, provided their Social Security numbers to ZOLL Medical. "But, looking to the First Circuit's guidance, such variations in what information was stolen (even the absence of specific allegations identifying what data was stolen), do not defeat standing. Notably, in Webb, [one plaintiff] satisfied the injury-in-fact element even though she was unable to offer specific allegations concerning what data had been lost in the IWP data breach." In re MOVEit Customer Data Sec. Breach Litig., 2024 WL 5092276, at *9 (D. Mass. Dec. 12, 2024) (citing Webb, 72 F.4th at 370); see also In re LastPass, 742 F. Supp. 3d at 121 (finding standing where "at least some stolen data was highly sensitive") (emphasis added).

Under the standard set forth in Webb, Plaintiffs plausibly plead material risk of future misuse of Private Information exposed in the Data Breach.

3. Other Alleged Harms Arising Out of the Data Breach

Plaintiffs allege several other harms that are coupled with either the actual financial fraud or the risk of future misuse, and ZOLL Medical argues that none of this harm is sufficient to establish injury-in-fact. The court agrees that the spam and diminution in value allegations are insufficient but finds that the allegations of emotional distress and lost benefit of the bargain are sufficiently concrete injuries for purposes of standing here.

a) Spam

ZOLL Medical argues that receiving increased spam emails or calls does not constitute injury-in-fact for standing purposes. Def.'s Mem. at 11-12 [Doc. No. 37]. Plaintiffs abandon any

argument to the contrary by failing to respond. In any event, Plaintiffs do not allege that their phone numbers or email addresses were exposed in the Data Breach. The court finds Plaintiffs' allegations of increased spam insufficient as injuries for purposes of standing.

b) Anxiety and Emotional Distress

ZOLL Medical argues that Plaintiffs' allegations of anxiety and emotional distress do not confer standing. Def.'s Mem. at 13-14 [Doc. No. 37]. In and of itself, this is true. See, e.g., Baysal v. Midvale Indem. Co., 2022 WL 1155295, at *4 (W.D. Wis. Apr. 19, 2022), aff'd, 78 F.4th 976 (7th Cir. 2023) (no standing for anxiety and emotional distress from disclosure of personal information where "plaintiffs have failed to plead a concrete, non-emotional harm, along with these emotional harms"). However, "the question in this case is not whether Plaintiffs' allegations of emotional distress, on their own, are sufficiently concrete to establish injuries in fact. Instead, it is whether allegations of emotional distress, coupled with the substantial risk of future harm, are sufficiently concrete to establish standing in a claim for damages." In re Mednax, 603 F. Supp. 3d at 1203. Because Plaintiffs have alleged a substantial risk of future misuse of their Private Information, the court finds that their allegations of

emotional distress—coupled with that risk—are sufficiently concrete injuries for standing purposes.[8]

c) Diminished Value of Private Information

ZOLL Medical argues that courts do not recognize diminution in the value of one's private information as a source of injury-in-fact. Def.'s Mem. at 13 (citing Taylor, 693 F. Supp. 3d at 101). Although the First Circuit has not addressed this specific question, see Webb, 72 F.4th at 374 n.5 (declining to address diminution-in-value argument for standing because it was waived), one court in this district has looked to other jurisdictions and found that "courts have consistently 'rejected allegations that the diminution in value of personal information can support standing,' particularly where [as here] the plaintiffs 'have not alleged that they attempted to sell their personal information or that, if they have, the data breach forced them to accept a decreased price for that information[.]'" Taylor, 693 F. Supp. 3d at 101 (quoting Cooper v. Bonobos, Inc., 2022 WL 170622, at *5 (S.D.N.Y. Jan. 19, 2022)). Plaintiffs point to courts in other jurisdictions that have recently departed from this concept of "selling" personal information on the market. See Opp. at 10 [Doc. No. 38]; see, e.g., In re Mednax, 603 F. Supp. 3d at 1204 (collecting cases, including In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 462

[8] The same analysis holds for loss of privacy as an injury-in-fact, which ZOLL Medical does not dispute. See, e.g., id. at 1205 ("Plaintiffs' claims of loss of privacy are sufficient to confer standing" where they are "under a substantial and imminent risk of future identify theft"); Bohnak v. Marsh & McLennan Companies, Inc., 79 F.4th 276, 286 (2d Cir. 2023) ("[E]xposure of [plaintiff's] private information—including her SSN and other PII—to an unauthorized malevolent actor . . . falls squarely within the scope of an intangible harm the Supreme Court has recognized as 'concrete.'"). Cf. Taylor v. UKG, Inc., 693 F. Supp. 3d 87, 100 (D. Mass. 2023) (no standing where loss of privacy was alleged as standalone injury, without allegations "that any third parties actually viewed or will imminently view their data").

(D. Md. 2020)). In In re Marriott, for example, the court rejected the concept that the value of consumer personal information is derived "solely (or even realistically) by its worth in some imagined marketplace where the consumer actually seeks to sell it to the highest bidder," because "the value of personal identifying information is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their personal identifying information." In re Marriott, 440 F. Supp. 3d at 462.

Under either approach, Plaintiffs fail to establish standing based on the diminished value of their Private Information. There is no question that their Private Information has economic value; that is why such information is stolen. But the Complaint focuses on the Private Information's "inherent" rather than economic value, and only makes the conclusory allegation that Plaintiffs' "information has inherent value that Plaintiff[s] [were] deprived of when [their] Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web." Compl. ¶¶ 102, 115, 130, 145, 160, 175, 189, 204, 219, 233 [Doc. No. 33]. Plaintiffs cite no case for the theory that the "inherent" value of Private Information is diminished by the mere fact that others might gain something from that information—particularly when Plaintiffs have lost none of that information's value. Plaintiffs have not alleged that they have ever attempted to sell their Private Information or that their ability to do so has been hampered by the Data Breach. See Taylor, 693 F. Supp. 3d at 101. Nor have they alleged that their buying power in the marketplace of credit has been diminished in ways comparable to plaintiffs in the cases they cite—for example, by alleging "that [their] credit score[s] ha[ve] been damaged[.]" In re Mednax, 603 F. Supp. 3d at

1201, 1204; see also, e.g., In re Marriott, 440 F. Supp. 3d at 462 ("Here Plaintiffs allege that they suffered lower credit scores as a result of the data breach and that fraudulent accounts and tax returns were filed in their names.").[9]

Therefore, Plaintiffs lack standing based on the diminished value of their Private Information.

d) Lost Benefit of the Bargain

Finally, ZOLL Medical argues that Plaintiffs cannot assert injuries based on a lost benefit of the bargain—i.e., that they "overpaid for a service that was intended to be accompanied by adequate data security." Compl. ¶ 264 [Doc. No. 33]. ZOLL Medical offers a straw-man argument by saying that no plaintiff "alleges their payment would have varied based on the level of data security that came with the product." Def.'s Mem. at 12 [Doc. No. 37]. But that is not the thrust of Plaintiffs' argument, which is that they would simply not have chosen ZOLL Medical's products or services or entrusted ZOLL Medical with their Private Information had they known ZOLL Medical's data security was inadequate. See, e.g., Compl. ¶ 344 [Doc. No. 33]; see also id. ¶ 340 ("In exchange [for healthcare services and implied promises to protect their Private Information], Plaintiffs and Members of the Class agreed to pay money for these services . . .").

Courts have found benefit-of-the-bargain theories of injury sufficient for standing purposes when they arise from the alleged breach of an explicit or implicit contract for data security. See In re Marriott, 440 F. Supp. 3d at 463-66 (collecting cases). That is what Plaintiffs allege here. See Compl. ¶ 350 [Doc. No. 33] (breach of implied contract claim). The cases cited

---

[9] Plaintiffs cite other cases about diminished value, see Opp. at 10-11 [Doc. No. 38], but the analyses there discussed the merits of claims, not standing.

by ZOLL Medical do not deal with similar allegations. See, e.g., Katz, 672 F.3d at 76 (discussing standing under state statutory claim for false advertising and misrepresentation arising under M.G.L. c. 93A). And ZOLL Medical's contention that "a majority of courts disallow" such theories, Def.'s Mem. at 12 [Doc. No. 37], is belied by the fact that the case it cites for this proposition reached a different conclusion on appeal. See Carlsen v. GameStop, Inc., 833 F.3d 903, 909 (8th Cir. 2016) (affirming dismissal on other grounds, but finding standing where plaintiff alleged devaluation of subscription because of compromised privacy protection).[10]

The court finds the Plaintiffs' allegations of a lost benefit of the bargain are sufficiently concrete injuries for standing purposes.

C. Redressability by Injunctive Relief[11]

As to redressability, Plaintiffs request injunctive relief that would require ZOLL Medical to strengthen its data security systems and monitoring procedures, submit to annual audits of such systems and procedures, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs. Compl. ¶¶ 299, 354, 362 [Doc. No. 33]. ZOLL Medical contends that Plaintiffs lack standing to pursue this relief because requiring ZOLL Medical to alter or improve its cybersecurity systems would not protect Plaintiffs from future misuse of their Private

[10] The court disregards ZOLL Medical's argument about a causal relationship being interrupted by "the independent actions of prescribing physicians," which comes from a line of summary judgment cases discussing proximate cause, not standing. See Sergeants Benevolent Ass'n Health & Welfare Fund v. Sanofi-Aventis U.S. LLP, 20 F. Supp. 3d 305, 325 (E.D.N.Y. 2014), aff'd, 806 F.3d 71 (2d Cir. 2015) (quoting UFCW Loc. 1776 v. Eli Lilly & Co., 620 F.3d 121, 135 (2d Cir. 2010)).

[11] ZOLL Medical does not dispute that damages would compensate Plaintiffs for their injuries.

Information, which is already in the hands of cybercriminals. Def.'s Mem. at 14-15 [Doc. No. 37].

ZOLL Medical cites the First Circuit's denial of standing to pursue similar injunctive relief in Webb, where "an injunction requiring [defendant] to improve its cybersecurity systems cannot protect the plaintiffs from future misuse of their PII by the individuals they allege now possess it." Id. at 14 (quoting Webb, 72 F.4th at 378). ZOLL Medical omits two significant departures from those facts here. First, unlike the defendant in Webb, ZOLL Medical experienced a subsequent cybersecurity incident that impacted employees' Private Information in December 2023, demonstrating the continued vulnerability to future misuse. Compl. ¶¶ 358-59 [Doc. No. 33]. Second, the Webb plaintiffs admitted that the defendant had "implemented new security safeguards to prevent and mitigate data breaches" after the breach at issue. Webb, 72 F.4th at 378. But Plaintiffs here specifically allege that ZOLL Medical did not "implement[] measures to protect Private Information" after the Data Breach. Compl. ¶ 360 [Doc. No. 33]. Plaintiffs are thus more likely to suffer future harm than the Webb plaintiffs. And that risk of future harm would, in turn, be redressable by requiring ZOLL Medical to take steps to protect Plaintiffs' information.

Accordingly, the court finds that Plaintiffs have standing.

III. Failure to State a Claim

The court turns to ZOLL Medical's challenges that Plaintiffs' causes of action fail to state a claim.[12]

A. Standard of Review

In evaluating a motion to dismiss for failure to state a claim, the court assumes "the truth of all well-pleaded facts" and draws "all reasonable inferences in the plaintiff's favor." Nisselson v. Lernout, 469 F.3d 143, 150 (1st Cir. 2006). To survive dismissal, a complaint must contain sufficient factual material to "state a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). "While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations . . . [f]actual allegations must be enough to raise a right to relief above the speculative level." Id. at 555 (citations omitted). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009).

B. Negligence

Plaintiffs allege that ZOLL Medical owed Plaintiffs a duty of care "to use reasonable means to secure and safeguard" their Private Information and provide data security consistent with industry standards; that ZOLL Medical breached that duty "by failing to adopt, implement, and maintain adequate security measures to safeguard that information"; and that this failure

[12] Because the parties principally apply Massachusetts law to the common law claims, see Opp. at 13 n.2 [Doc. No. 38], the court assumes for purposes of this motion that the common law claims require the same elements in each jurisdiction, except where otherwise specified.

caused the theft and misuse of Plaintiffs' Private Information, including the consequential harms discussed in the court's standing analysis above. See Compl. ¶¶ 285, 288, 291, 293-296 [Doc. No. 33].

1. Duty Under Illinois Law

ZOLL Medical argues that the negligence claim under Illinois law must fail because Illinois does not recognize a common law duty to protect personal information. Def.'s Mem. at 18 [Doc. No. 37]. But the sole case ZOLL Medical cites for this proposition, Perdue v. Hy-Vee, Inc., 455 F. Supp. 3d 749, 759 (C.D. Ill. 2020), relied on an Illinois case that has since been superseded by statute, as recognized in Flores v. Aon Corp., 2023 IL App (1st) 230140, ¶ 23, 242 N.E.3d 340; see also 815 Ill. Comp. Stat. Ann. 530/45(a) ("A data collector that . . . maintains or stores . . . records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access . . ."). Perdue therefore provides no basis for dismissing Plaintiffs' negligence claim under Illinois law.

2. Economic Loss Rule

The court addresses next the economic loss rule, which ZOLL Medical contends bars recovery here. The court finds that the rule does not bar Plaintiffs' claims except as to Kansas law, a conclusion Plaintiffs fail to oppose.

a) Massachusetts

"Massachusetts, which is not alone, holds that 'purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage.'" In re TJX Companies Retail Sec. Breach Litig., 564 F.3d 489, 498 (1st Cir. 2009), as amended on

reh'g in part (May 5, 2009) (quoting Aldrich v. ADD Inc., 437 Mass. 213, 222, 770 N.E.2d 447 (2002)). However, Massachusetts "ha[s] not applied the economic loss rule to claims of negligence by a fiduciary" but to cases where "the parties usually were in a position to bargain freely concerning the allocation of risk, and, more importantly, there was no fiduciary relationship." Clark v. Rowe, 428 Mass. 339, 342, 701 N.E.2d 624 (1998); see also Szulik v. State St. Bank & Tr. Co., 935 F. Supp. 2d 240, 271 n.11 (D. Mass. 2013) (citing same). The economic loss doctrine generally applies to data breach cases between non-fiduciaries. See, e.g., Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 455 Mass. 458, 469, 918 N.E.2d 36 (2009) (rejecting argument by card-issuing credit unions that theft of credit card information from retailer amounted to physical harm to tangible property so as to overcome economic loss rule); In re TJX Companies, 564 F.3d at 470 (same); see also In re LastPass, 742 F. Supp. 3d at 128 (finding mere reliance on another's "purported cybersecurity expertise and its promises to keep their data safe" is insufficient to form a fiduciary relationship to avoid the rule).

But Massachusetts superior courts, acknowledging there is "no appellate authority directly on point," have declined to apply the economic loss rule "where patients are required to provide highly sensitive PII to a hospital to obtain medical care, are powerless to protect that information but rely on the hospital to do so consistent with state and federal law, and the hospital should reasonably have foreseen and guarded against the risk of disclosure." Shedd v. Sturdy Mem'l Hosp., Inc., 2022 WL 1102524, at *8 (Mass. Super. Apr. 5, 2022). Courts in this district have rejected the application of the economic loss doctrine in data breach cases where the plaintiffs adequately alleged a fiduciary duty by the holder of their private and confidential information. See, e.g., In re Shields Health Care Grp., Inc. Data Breach Litig., 721 F. Supp. 3d

152, 160-61 (D. Mass. 2024) (data breach claim sounding in negligence against provider of medical services); Doe v. Tenet Healthcare Corp., 731 F. Supp. 3d 142, 148 (D. Mass. 2024) (same). One court predicts that Massachusetts appellate courts would likely not apply the economic loss rule to "a claim for negligence based on the theft and misuse of employees' PII that they entrusted to their employer as a condition of employment." Portier v. NEO Tech. Sols., 2019 WL 7946103, at *18 (D. Mass. Dec. 31, 2019), report and recommendation adopted, 2020 WL 877035 (D. Mass. Jan. 30, 2020). Under Massachusetts law, a "special relationship" that gives rise to a fiduciary duty may be inferred where "a defendant reasonably could foresee that he would be expected to take affirmative action to protect the plaintiff and could anticipate harm to the plaintiff from the failure to do so." Adams v. Cong. Auto Ins. Agency, Inc., 90 Mass. App. Ct. 761, 765, 65 N.E.3d 1229 (2016) (citation omitted). The Portier court found a special relationship between plaintiff employees and defendant employers because the employers "had exclusive control over their employees' PII that it collected and stored" and the employees, "who were powerless to protect their PII, relied on [employers] to safeguard their PII from cyber thieves, and [employers] should have reasonably foreseen the harm that befell Plaintiffs when it failed to adequately secure their PII[.]" Portier, 2019 WL 7946103, at *21 (internal quotation marks and citations omitted).

Here, Plaintiffs allege they entrusted their Private Information to ZOLL Medical either "as a condition of [their] employment," Compl. ¶¶ 139, 227 [Doc. No. 33], or "as a condition of receiving products and services from Zoll." Id. ¶ 41. Although Plaintiffs were not patients of ZOLL Medical and ZOLL Medical is not a direct medical services provider, ZOLL Medical could reasonably foresee from the nature of its products and services that it would be expected to

take affirmative action to protect Plaintiffs' Private Information and could anticipate harm to Plaintiffs in the absence of such action. See Adams, 90 Mass. App. Ct. at 765. The ZOLL Medical products and services Plaintiffs used were medically prescribed "advanced emergency care devices." Compl. ¶¶ 2, 96, 109, 124, 154, 183, 198, 213 [Doc. No. 33]. Plaintiffs' Private Information was "transmitted through Zoll's medical devices for purposes of monitoring and diagnostic analysis." Id. ¶ 34. Plaintiffs allege that the exposed data disclosed their medical conditions, with "some of the data . . . linked to medical equipment associated with specific medical conditions." Id. ¶ 4. And Plaintiffs allege that ZOLL Medical "recognizes that it is a business associate under HIPAA and agrees that it will comply with HIPAA." Id. ¶¶ 87 & n.20.

Taken as a whole, the Complaint plausibly alleges that ZOLL Medical had a special relationship with Plaintiffs, who surrendered control of their Private Information to ZOLL Medical as a condition of their employment or use of prescribed ZOLL Medical devices. Because this special relationship gives rise to a fiduciary duty, the economic loss rule does not bar Plaintiffs' negligence claim under Massachusetts law.

b) Pennsylvania and Illinois

The analysis is much the same in Pennsylvania and Illinois. The Portier court reached its conclusion about the likely application of Massachusetts law to a data breach case based on the "legal parallels" between Massachusetts and Pennsylvania's economic loss rules. See Portier, 2019 WL 7946103, at *18-21; Dittman v. UPMC, 649 Pa. 496, 499, 196 A.3d 1036 (2018) ("under Pennsylvania's economic loss doctrine, recovery for purely pecuniary damages is permissible under a negligence theory provided that the plaintiff can establish the defendant's

breach of a legal duty arising under common law that is independent of any duty assumed pursuant to contract").

In Illinois, the "[economic loss] doctrine is founded on the theory that 'parties to a contract may allocate their risks by agreement and do not need the special protections of tort law to recover damages caused by a breach of contract.'" Flores, 2023 IL App (1st) 230140, ¶ 56 (citation omitted). Thus, "[w]here a duty arises outside of the contract, the economic loss doctrine does not prohibit recovery in tort for the negligent breach of that duty." Congregation of the Passion, Holy Cross Province v. Touche Ross & Co., 159 Ill. 2d 137, 162, 636 N.E.2d 503 (1994); see also Flores, 2023 IL App (1st) 230140, ¶ 56 (applying Congregation of the Passion in data breach case, where injury arose from alleged breach of common law duty to safeguard personal information and not from express contract).

For reasons similar to those discussed for Massachusetts, the economic loss rule does not bar Plaintiffs' negligence claim under Pennsylvania and Illinois law.

c) Florida, Texas, and New York

The economic loss rule is not a bar under Florida, Texas, and New York law for an additional reason: in those states, the rule only applies in product liability cases. See Tiara Condo Ass'n, Inc. v. Marsh & McLennan Cos., Inc., 110 So. 3d 399, 407 (Fla. 2013) ("the economic loss rule applies only in the products liability context"); Sharyland Water Supply Corp. v. City of Alton, 354 S.W.3d 407, 418 (Tex. 2011) ("[W]e have applied the economic loss rule only in cases involving defective products or failure to perform a contract."); Thawar v. 7-Eleven, Inc., 165 F. Supp. 3d 524, 532 (N.D. Tex. 2016) (discussing Sharyland in data breach case); Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 749 (S.D.N.Y. 2017) (data breach case declining

to apply New York's economic loss rule outside the context of products liability and where plaintiff alleges "a legal duty independent of the contract itself has been violated") (citations omitted). Because this is not a product liability action, the economic loss rule does not apply under these states' laws.

d) Kansas

Plaintiffs fail to oppose ZOLL Medical's argument as to Kansas law. See Opp. at 14, 16-17 [Doc. No. 38] (asserting "[t]he economic loss doctrine does not bar Plaintiffs' claim" but addressing only Massachusetts law and "[t]he laws of Florida, Illinois, New York, Pennsylvania, and Texas"). Therefore, any opposition to this argument is deemed waived. See Schneider v. Local 103 I.B.E.W. Health Plan, 442 F.3d 1, 3 (1st Cir. 2006); see also Nikijuluw v. Gonzales, 427 F.3d 115, 120 n. 3 (1st Cir. 2005) ("It is well established that 'issues adverted to in a perfunctory manner, unaccompanied by some effort at developed argumentation, are deemed waived.'") (citation omitted).

Accordingly, this court grants ZOLL Medical's motion to dismiss Plaintiffs' negligence claim only as to Kansas law.

3. Damages

Finally, ZOLL Medical argues that Plaintiffs fail to plead compensable damages as required to state a negligence claim. Def.'s Mem. at 16 [Doc No. 37]. This argument relies principally on cases in which data breach plaintiffs failed to plead economic or out-of-pocket costs. See Krottner v. Starbucks Corp., 406 F. App'x 129, 131 (9th Cir. 2010) (dismissing claim under Washington law because "the only plaintiff who claims his personal information has been misused, alleges no loss related to the attempt to open a bank account in his name"); In re

SuperValu, Inc., 2018 WL 1189327, at *12 (D. Minn. Mar. 7, 2018) (dismissing claim under Illinois law because plaintiff alleged only that he "noticed a fraudulent charge on his credit card statement and immediately cancelled his credit card," and did not allege that he incurred out-of-pocket costs).

As discussed above, some of the named Plaintiffs allege actual incidents of financial fraud. Compl. ¶¶ 116, 131, 146, 161, 190, 205 [Doc. No. 33]. They further allege that these incidents "caused financial strain," id., but they include no specific allegations, such as detailing out-of-pocket costs, to support the conclusory allegation as to damages already incurred.[13]

Plaintiffs also allege the loss of "considerable time and money" on an ongoing basis to mitigate and address future harms resulting from the Data Breach. Id. ¶¶ 265-66. These facts are sufficient to survive a motion to dismiss. See Weekes v. Cohen Cleary P.C., 723 F. Supp. 3d 97, 103 (D. Mass. 2024) (finding sufficient allegations of "either actual misuse of plaintiff's PII or that another victim of the breach has had his or her PII misused, along with other indicia of imminent harm"); In re Shields, 721 F. Supp. 3d at 161 ("Where Plaintiffs show a substantial risk of harm manifesting in the future, the 'element of injury and damage will have been satisfied and the cost of that monitoring is recoverable in tort.'") (citation omitted).

[13] Plaintiffs argue that they have "alleged out-of-pocket costs for protective measures, such as credit monitoring fees, credit report fees, [and] credit freeze fees." Opp. at 17 [Doc. No. 38]. But the Complaint only alleges that Plaintiffs "may also incur" such costs, Compl. ¶ 262 (emphasis added) [Doc. No. 33], not that such costs have actually been or are likely to be incurred.

Plaintiffs have sufficiently pleaded damages to survive a motion to dismiss their negligence claim.[14]

C. Negligence Per Se

Plaintiffs voluntarily dismiss their negligence per se cause of action. See Opp. at 13 n.1 [Doc. No. 38].

D. Breach of Fiduciary Duty

ZOLL Medical argues that Plaintiffs' breach of fiduciary duty claim fails because no such duty can be alleged. For the reasons already discussed above with regard to the economic loss doctrine, the court finds Plaintiffs have plausibly alleged a special relationship so as to constitute a fiduciary duty under Massachusetts law, where Plaintiffs furnished their Private Information to ZOLL Medical as a condition of employment or receiving prescribed medical devices; ZOLL Medical had exclusive control over the Private Information it collected; and Plaintiffs relied on ZOLL Medical to protect that Private Information. Accordingly, the court finds this claim survives ZOLL Medical's motion to dismiss.

E. Unjust Enrichment

1. Adequate Remedy at Law

ZOLL Medical argues that the unjust enrichment claim must be dismissed because "'a party with an adequate remedy at law cannot claim unjust enrichment'. . . . [i]t is the availability

[14] ZOLL Medical's brief argues in passing that Plaintiffs failed to plead causation. See Def.'s Mem. at 18 [Doc. No. 37] (referring back to the traceability issue for standing). The court addressed traceability in the discussion above; any different causation argument as to the negligence cause of action is waived. See United States v. Zannino, 895 F.2d 1, 17 (1st Cir. 1990).

of a remedy at law, not the viability of that remedy, that prohibits a claim for unjust enrichment." Def.'s Mem. at 20 [Doc. No. 37] (quoting Shaulis v. Nordstrom, 865 F.3d 1, 16 (1st Cir. 2017)); see also Tomasella v. Nestle USA, Inc., 962 F.3d 60, 82 (1st Cir. 2020) (same). As the First Circuit explained in Tomasella, however, "despite the mutual exclusivity of damages for breach of contract and unjust enrichment, 'it is accepted practice to pursue both theories at the pleading stage.'" 962 F.3d at 84 (quoting Lass v. Bank of America, N.A., 695 F.3d 129, 140 (1st Cir. 2012)). The Tomasella court explained further that Shaulis and Lass were not in conflict, where in the former, there was no ambiguity that a contract existed, so plaintiff could not assert a contract claim in addition to an unjust enrichment claim, while in the latter there was an ambiguity casting doubt on the availability of a contract claim, such that the plaintiff was permitted to proceed on both theories at the pleading stage. Id.

Here, the availability of Plaintiffs' implied contract claim is disputed. Accordingly, unjust enrichment may provide an alternative remedy at law.

2. Conferral of a Benefit

Plaintiffs allege that "[p]art of the price [they] paid to Defendants and/or Defendants' healthcare partners was intended to be used by Defendants to fund adequate security of their computer system(s) and Plaintiffs' . . . Private Information[,]" but ZOLL Medical "instead calculated to avoid their data security obligations . . . by utilizing cheaper, ineffective security measures" and thus "enriched itself by saving the costs they reasonably should have expended on data security measures." Opp. at 21 [Doc. No. 38]; Compl. ¶¶ 264, 314 [Doc. No. 33]. ZOLL Medical argues that these allegations are not sufficient to plausibly allege that Plaintiffs conferred an economic benefit on ZOLL Medical, where Plaintiffs do not allege they paid

"'extra for a security package that they were promised and did not receive.'" Def.'s Mem. at 21 [Doc. No. 37] (quoting Webb v. Injured Workers Pharmacy, LLC, 2023 WL 5938606, at *4 (D. Mass. Sept. 12, 2023) ("Webb II")).[15] In stating this extra-payment requirement, the Webb II court relied on a District of Minnesota's court's decision in In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014), concerning a breach of payment-card security. But while that court rejected an "overcharge" theory, it did so based on the specific factual allegations in that case that are not present here: Target's customers paid the same price for goods that were purchased by cash or credit, rendering the theory that Target had overcharged for data security as to the card-purchases implausible. Id. at 1178.

Moreover, the In re Target court distinguished its facts from Resnick v. AvMed, Inc., where the court found a plausible claim based on plaintiffs' allegations that monthly premiums paid to a healthcare insurer were used to "pay for the administrative costs of data management and security." Resnick v. AvMed, Inc., 693 F.3d 1317, 1328 (11th Cir. 2012). Significantly, there was no allegation in Resnick that the insureds paid a separate premium for increased data security. Similarly, in Tenet, another court in this district found unjust enrichment allegations sufficient where plaintiff "paid for medical services from [defendant] with the expectation that

[15] ZOLL Medical also argues that Plaintiffs do not allege they "paid anything at all," Def.'s Mem. at 21 [Doc. No. 37]. Plaintiffs refer throughout the Complaint to "the price [they] paid to Defendants and/or Defendants' healthcare partners," e.g. Compl. ¶ 264 [Doc. No. 33], and it is reasonable for the court to infer that actual payment was made. See Nisselson, 469 F.3d at 150 (court must draw "all reasonable inferences in the plaintiff's favor"). To the extent ZOLL Medical suggests that any payments would have flowed through intermediaries such as "healthcare partners" or insurers, that does not undermine the fact that Plaintiffs' transactions resulted in the conferral of such a benefit on ZOLL Medical.

her health information would remain confidential, and not disclosed for [defendants'] benefit, for marketing purposes, or for sale or trade with third parties." Tenet, 731 F. Supp. 3d at 151.

The court finds the facts alleged here similar to those in Resnick and Tenet, and distinguishable from the equivalent cash payment circumstances in In re Target, which Webb II found persuasive. Plaintiffs have adequately alleged a theory for unjust enrichment based on their expectation of how their payments would be used.

Accordingly, this claim survives ZOLL Medical's motion to dismiss.[16]

F. Breach of Implied Contract

ZOLL Medical argues that the breach of implied contract claim should be dismissed for failure to allege breach or damages. Because the Complaint is unclear about whether an implied-in-fact or implied-in-law contract is at issue, the court considers both.

1. Implied-in-Fact Contract

"In the absence of an express agreement, a contract implied in fact may be found to exist from the conduct and relations of the parties." Jackson v. Action for Bos. Cmty. Dev., Inc., 403 Mass. 8, 9, 525 N.E.2d 411 (1988) (citation omitted). Courts will construe a breach of contract claim as one for an implied-in-fact contract where a plaintiff "argue[s] principally that it reached an actual, enforceable agreement with [defendant] that was implied by the dealings of the two parties." Mass. Eye & Ear Infirmary v. QLT Phototherapeutics, Inc., 412 F.3d 215, 230 (1st Cir.

---

[16] ZOLL Medical also argues that any benefit it received cannot be "unjust" because Plaintiffs were prescribed life-saving medical devices. Def.'s Mem. at 21 [Doc. No. 37]. But the determination of justness or unjustness turns on "[c]onsiderations of equity and morality" and "the reasonable expectations of the parties[,]" Metro. Life Ins. Co. v. Cotter, 464 Mass. 623, 644 (2013) (citations omitted), and "cannot be decided on a motion to dismiss," Shedd, 2022 WL 1102524, at *11.

2005). This is because "[a] contract implied in fact requires the same elements as an express contract and differs only in the method of expressing mutual assent." Id. (citation omitted). "Courts have recognized that implied contract claims can be based on promises made in websites," but "to support a claim for breach of an implied-in-fact contract, Plaintiffs must allege sufficient facts to permit an inference that the parties reciprocally agreed to enter into an agreement based on the online privacy statement." In re Shields, 721 F. Supp. 3d at 163 (collecting cases).

The Complaint alleges a "meeting of the minds" based on ZOLL Medical's privacy policy. See, e.g., Compl. ¶¶ 342-45 [Doc. No. 33]. ZOLL Medical points to the privacy policy itself, in which ZOLL Medical states only that it will "undertake reasonable efforts to protect [Plaintiffs'] personal information" but "cannot guarantee its security." Def.'s Mem. at 23 [Doc No. 37]; Compl. ¶ 40 [Doc No. 33] (citing Privacy Policy, ZOLL Med. Corp., https://zoll.com/privacy-policy). Plaintiffs respond by pointing to other legal obligations (as discussed below). The court finds that Plaintiffs have not stated a claim for breach of an implied-in-fact contract where they have not alleged sufficient facts that "the parties reciprocally agreed to enter into an agreement based on the online privacy statement," In re Shields, 721 F. Supp. 3d at 163, aside from conclusory language about a "meeting of the minds," Compl. ¶ 345 [Doc No. 33].

2. Implied-in-Law Contract

"A quasi contract or a contract implied in law is an obligation created by law for reasons of justice, without any expression of assent and sometimes even against a clear expression of dissent." Metro. Life Ins. Co. v. Cotter, 464 Mass. 623, 643, 984 N.E.2d 835 (2013) (citation and

internal quotation marks omitted). "The injustice of the enrichment or detriment in quasi-contract equates with the defeat of someone's reasonable expectations." Salamon v. Terra, 394 Mass. 857, 859, 477 N.E.2d 1029 (1985) (citing 1 A. Corbin, Contracts § 19 (1963)). In the data breach context, courts have allowed breach of implied-in-law contract claims where "Plaintiffs' expectations of data security were reasonable given the federal laws that govern handling private information." See, e.g., In re Shields, 721 F. Supp. 3d at 163 (citing HIPAA and FTC requirements); see also Tenet Healthcare Corp., 731 F. Supp. 3d at 150 (patient had reasonable expectation that confidential health or personal data transferred to healthcare provider would be kept private pursuant to HIPAA and privacy policies). Cf. Doe v. Emerson Hosptial, 2023 WL 8869624, at *4 (Mass. Super. Nov. 22, 2023) (denying motion to dismiss implied contract in data breach case, collecting cases from other jurisdictions, and noting "the absence of case law from the Commonwealth clearly on point").

Plaintiffs allege that they relied on the reasonable expectations of Plaintiffs based on laws and regulations like HIPAA. See, e.g., Compl. ¶ 338 [Doc No. 33]. They argue that ZOLL Medical promised to "'reasonably protect such information' in accordance with industry standards and relevant laws and regulations, including HIPAA and the FTC Act." Opp. at 23 [Doc. No. 38] (citing Compl. ¶¶ 336, 337, 348 [Doc No. 33]); see also Compl. ¶ 40 (describing privacy policy as "[r]ecognizing [ZOLL Medical's] legal and equitable duties"). The court finds that Plaintiffs have alleged an implied-in-law contract. Because Plaintiffs received prescription medical devices from ZOLL Medical, "a business associate under HIPAA [that] agrees that it will comply with HIPAA," Compl. ¶¶ 87 & n.20 [Doc. No. 33], and is allegedly subject to other applicable data security laws such as the FTC Act, id. ¶¶ 71-77, Plaintiffs have alleged a

reasonable expectation that ZOLL Medical would protect their information according to those standards. Such an expectation was further evidenced by the privacy policy's commitment to take "reasonable efforts to protect" that information. Id. ¶ 40 (citing Privacy Policy, ZOLL Med. Corp., https://zoll.com/privacy-policy). These allegations are sufficient to state an implied-in-law obligation for ZOLL Medical to comply with such standards, and Plaintiffs plausibly allege that ZOLL Medical's non-compliance breached this obligation. See In re Shields, 721 F. Supp. 3d at 163; Tenet Healthcare Corp., 731 F. Supp. 3d at 150.

3. Damages

As the court finds that Plaintiffs' claim is for an implied-in-law contract, the damages available to Plaintiffs are in the nature of restitution. "In such a case [implied-in-law contract], the proper measure of damages is quantum meruit, or the reasonable value of services provided." Incase Inc. v. Timex Corp., 488 F.3d 46, 54 (1st Cir. 2007) (citing J.A. Sullivan Corp. v. Mass., 397 Mass. 789, 494 N.E.2d 374 (1986)); see also Salamon, 394 Mass. at 859 ("The underlying basis for awarding quantum meruit damages in a quasi-contract case is unjust enrichment of one party and unjust detriment to the other party.") (citation omitted).

ZOLL Medical makes the cursory argument that "[a]s noted above, plaintiffs do not allege actionable damage," Def.'s Mem. at 23 [Doc. No. 37], without specifying what argument "above" they refer to. "It is not enough merely to mention a possible argument in the most skeletal way, leaving the court to do counsel's work, create the ossature for the argument, and put flesh on its bones." Zannino, 895 F.2d at 17. In any event, the court has explained above that Plaintiffs plausibly allege that ZOLL Medical was unjustly enriched through payments Plaintiffs made for ZOLL Medical's products, payments they expected to be directed in part toward

compliance with the applicable data security standards. For the same reason, they have plausibly alleged damages for their implied-in-law contract claim.

The Complaint makes the conclusory allegation that the employee Plaintiffs (Gerth and Weese) "paid for the provided services in exchange for . . . employment and the protection of their Private Information." Compl. ¶ 345 (emphasis added) [Doc. No. 33]. This statement suggests the employee Plaintiffs even paid for their own employment, which is implausible. These are not "well-pleaded facts," and the court need not assume their truth for purposes of this motion. See Nisselson, 469 F.3d at 150. The Complaint fails to otherwise explain how the employee Plaintiffs can state damages under the implied-in-law contract claim. Thus, the court finds that Plaintiffs Gerth and Weese have not stated a breach of implied-in-law contract claim.

The breach of implied contract claim is therefore dismissed as an implied-in-fact contract, and as to Plaintiffs Gerth and Weese as an implied-in-law contract. It is otherwise allowed as a breach of implied-in-law contract claim by the remaining Plaintiffs.

G. Declaratory and Injunctive Relief

ZOLL Medical argues that Plaintiffs' cause of action for declaratory and injunctive relief under the Declaratory Judgment Act, 28 U.S.C. § 201, should also be dismissed because it is duplicative of the negligence cause of action. Def.'s Mem. at 23-24 [Doc. No. 37]. The court agrees.

"[C]ourts have broad discretion to decline to enter a declaratory judgment" under the Declaratory Judgment Act. DeNovellis v. Shalala, 124 F.3d 298, 313 (1st Cir. 1997) (citing Wilton v. Seven Falls Co., 515 U.S. 277, 287 (1995)); see also Green v. Mansour, 474 U.S. 64, 72 (1985) (noting that the Declaratory Judgment Act "confers a discretion on the courts rather

than an absolute right upon the litigant"). Although "the existence of another adequate remedy does not preclude a declaratory judgment that is otherwise appropriate," Fed. R. Civ. P. 57, courts will dismiss a claim as duplicative if "[p]leading an additional cause of action provides [the plaintiff] with no further remedy." Young v. Wells Fargo Bank, N.A., 717 F.3d 224, 237 (1st Cir. 2013); see, e.g., Transpac Marine, LLC v. Yachtinsure Servs., Inc., 655 F. Supp. 3d 18, 29 (D. Mass. 2023) (finding moot redundant declaratory judgment counterclaims).

Plaintiffs argue their declaratory judgment claim is not duplicative because it seeks injunctive relief. But that injunctive relief is also duplicative. Plaintiffs request that the court order ZOLL Medical to provide lifetime credit monitoring and identity theft insurance to Plaintiffs, and implement and maintain reasonable security and monitoring measures for Private Information, including submitting to periodic third-party security audits. Compl. ¶¶ 355-365 [Doc. No. 33]. The substance of this request is no different from the injunctive relief sought in Plaintiff's negligence or breach of implied contract causes of action. See id. ¶¶ 299, 354.

The declaratory and injunctive relief cause of action is therefore dismissed as duplicative.

H. Florida Deceptive and Unfair Trade Practices Act

The FDUTPA provides a civil cause of action for "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204. "A consumer claim for damages under FDUTPA has three elements: (1) a deceptive act or unfair practice; (2) causation; and (3) actual damages." City First Mortg. Corp. v. Barton, 988 So. 2d 82, 86 (Fla. Dist. Ct. App. 2008) (citation omitted).

ZOLL Medical seeks dismissal of the FDUTPA claim, arguing that the Florida Plaintiffs fail to: (1) establish a sufficient nexus to the state of Florida; (2) plead with sufficient particularity under Rule 9(b); and (3) plead actual damages.

1. Nexus

As to nexus, the FDUTPA "prohibit[s] unfair, deceptive and/or unconscionable practices which have transpired within the territorial boundaries of [Florida] without limitation." Millennium Commc'ns & Fulfillment, Inc. v. Off. of Att'y Gen., Dep't of Legal Affs., State of Fla., 761 So. 2d 1256, 1262 (Fla. Dist. Ct. App. 2000). Courts have construed FDUTPA to apply "only to action that occurred within the state of Florida," but "the statute does not limit its protection to acts occurring exclusively in Florida." Eli Lilly & Co. v. Tyco Integrated Sec., LLC., 2015 WL 11251732, at *4 (S.D. Fla. Feb. 10, 2015) (collecting cases) (emphasis added).

Eli Lilly is instructive. There, defendants based in Florida provided premises security and monitoring equipment for a distribution warehouse in Connecticut, which was burglarized using surveillance vulnerabilities identified in a confidential system proposal created by defendants. Id. at *1. Although the burglary occurred outside Florida, the court found a sufficient relationship with the state of Florida because plaintiffs' complaints about defendants' "failure to diligently assess its ability to safeguard [plaintiff's] information, as well as representations made concerning this ability, is conduct that actually occurred in, or, at a minimum, flowed from business practices occurring within the State of Florida." Id. at *5.

Similarly here, although the cyberattack, like the burglary in Eli Lilly, occurred outside Florida, the challenged conduct, like the "business practices" in Eli Lilly, occurred within Florida, where ZOLL Medical "advertised, offered, or sold goods or services in Florida," which

included allegedly misrepresenting to Florida Plaintiffs "that it would protect the privacy and confidentiality" of their Private Information and "comply with common law and statutory duties" pertaining to such security and privacy. Compl. at 75-77 ¶¶ 202-03 [Doc. No. 33].[17] The alleged misrepresentations and omissions "were likely to deceive reasonable consumers about the adequacy of Zoll's data security and ability to protect the confidentiality of consumers' Private Information." Id. at 77 ¶ 204. As alleged, this allowed ZOLL Medical to retain consumers who otherwise would have sought goods and services from competitors. Id. at 77 ¶ 206. All this suffices to establish a nexus with Florida for purposes of the FDUTPA.[18]

2. Rule 9(b)

Next, ZOLL Medical contends that the FDUTPA claim fails because it must be pleaded with particularity under Rule 9(b). Federal courts are split as to the relationship between the FDUTPA and Rule 9(b)'s heightened pleading requirement: some courts apply Rule 9(b) when an FDUTPA claim sounds in fraud, whereas other courts decline to apply Rule 9(b) to any FDUTPA claim. See Eli Lilly, 2015 WL 11251732, at *2-4 (collecting cases and discussing split).

---

[17] The paragraph numbering in the Complaint restarts at 199 from page 75 onward. To avoid confusion, the court cites to both page and paragraph numbers for all paragraphs incorrectly numbered.

[18] ZOLL Medical's cases are not to the contrary. In Toretto v. Donnelley Fin. Sols., Inc., 583 F. Supp. 3d 570, 606 (S.D.N.Y. 2022), the parties agreed that the only connection to Florida was that the injured party was a Florida resident; similarly, in Hakim-Daccach v. Knauf Int'l GmbH, 2017 WL 5634629, at *7 (S.D. Fla. Nov. 22, 2017), the alleged wrongdoing was only "indirectly associated with bank accounts in Miami."

The rationale for the latter approach is that the "FDUTPA was enacted to provide remedies for conduct outside the reach of traditional common law torts such as fraud." Harris v. Nordyne, LLC, 2014 WL 12516076, at *4 (S.D. Fla. Nov. 14, 2014) (quoting Guerrero v. Target Corp., 889 F. Supp. 2d 1348, 1355 (S.D. Fla. 2012) (emphasis added)); see also State, Off. of Atty. Gen., Dep't of Legal Affs. v. Wyndham Int'l, Inc., 869 So. 2d 592, 598 (Fla. Dist. Ct. App. 2004) ("A deceptive or unfair trade practice [under the FDUTPA] constitutes a somewhat unique tortious act because, although it is similar to a claim of fraud, it is different in that, unlike fraud, a party asserting a deceptive trade practice claim need not show actual reliance on the representation or omission at issue."). Moreover, "requiring plaintiffs to plead FDUTA claims with particularity would not advance the primary goals of Rule 9(b). FDUTPA's elements are more particularized than those of common law fraud. A complaint which states plausible allegations of a deceptive or unfair practice in the course of trade or commerce and resultant damages will generally put a FDUTPA defendant on fair notice of the nature of plaintiff's claim and the grounds upon which it is based, without the risk of subjecting the defendant to specious claims of impropriety." Eli Lilly, 2015 WL 11251732, at *4 (internal citations omitted).

The court is persuaded by this approach and finds that the Rule 9(b) heightened pleading standard does not apply to the Florida Plaintiffs' FDUTPA claim.

3. Damages

Finally, ZOLL Medical contends that the Florida Plaintiffs fail to allege damages cognizable under the FDUTPA because their mitigation-related injuries—e.g., the time and out-of-pocket costs spent mitigating harm from or preventing future harm from the Data Breach, see Compl. ¶ 207 [Doc No. 33]—are only consequential and not directly "attributable to the

diminished value of the goods or services received" in the form of a prescribed medical device. Def.'s Mem. at 25 (quoting In re Brinker Data Incident Litig., 2020 WL 691848, at *13 (M.D. Fla. Jan. 27, 2020)); see also Rollins, Inc. v. Heller, 454 So. 2d 580, 585 (Fla. Dist. Ct. App. 1984) (defining "actual damages" for purposes of the FDUTPA as "the difference in the market value of the product or service in the condition in which it was delivered and its market value in the condition in which it should have been delivered according to the contract of the parties").

Plaintiffs appear to concede this by highlighting only one aspect of the damages the Florida Plaintiffs seek under the FDUTPA: the overpayment for ZOLL Medical's goods and services. Opp. at 27 [Doc. No. 38]; Compl. at 77 ¶ 207 [Doc. No. 33]. In other words, the medical devices Florida Plaintiffs ordered from ZOLL Medical "were not delivered in the form promised (sufficiently safeguarding consumers' Private Information)." Opp. at 27 [Doc. No. 38]. The collection of Plaintiffs' Private Information was intertwined with their use of the medical devices. See, e.g., Compl. ¶ 34 (Private Information "transmitted through Zoll's medical devices for purposes of monitoring and diagnostic analysis.") [Doc. No. 33]. A reasonable factfinder could find that the safeguarding of that Private Information was part of the bargain Plaintiffs paid for, and as the court explained above, Plaintiffs plausibly allege that they made payments with the expectation that part of those funds would go toward data security.

The court therefore finds that Plaintiffs have stated a claim for damages under the FDUTPA.

4. Injunctive Relief

Florida Plaintiffs' FDUTPA claim also survives because they seek injunctive relief. Under the FDUTPA, injunctive relief is available "[w]ithout regard to any other remedy or relief

to which a person is entitled." Fla. Stat. § 501.211(1); see also Galstaldi v. Sunvest Communities USA, LLC, 637 F. Supp. 2d 1045, 1057 (S.D. Fla. 2009) ("declaratory relief is available regardless of whether an adequate remedy at law also exists"). Florida courts have found the statute to be "clear on its face. It merely requires an allegation that the consumer is in a position to complain (that he or she is aggrieved by the alleged violation) and that the violation has occurred, is now occurring, or is likely to occur in the future." Davis v. Powertel, Inc., 776 So. 2d 971, 975 (Fla. Dist. Ct. App. 2000). Thus, it is "broadly worded to authorize declaratory and injunctive relief even if those remedies might not benefit the individual consumers who filed the suit." Id.

The court therefore finds Florida Plaintiffs have stated a claim under the FDUTPA for injunctive relief.

I. Kansas Consumer Protection Act

Under the KCPA, "[n]o supplier shall engage in any deceptive act or practice in connection with a consumer transaction." Kan. Stat. § 50-626(a). "The KCPA provides that an 'aggrieved consumer' may maintain a private right of action against a supplier if: (1) the supplier willfully failed to state a material fact; or (2) the supplier willfully failed to state, concealed, suppressed, or omitted a material fact." Stechschulte v. Jennings, 297 Kan. 2, 27-28, 298 P.3d 1083 (2013) (citing Kan. Stat. §§ 50-626(b)(3), 50-634(a)).

ZOLL Medical seeks to dismiss Plaintiff Becker's claim under the KCPA on the ground that the allegations fail to meet the heightened pleading standard of Rule 9(b). Def.'s Mem. at 26-27 [Doc No. 37] (citing In re MGC Health Data Sec. Issue Litig., 2023 WL 3057428, at *9 (W.D. Wash. Mar. 27, 2023), report and recommendation adopted, 2023 WL 4131746 (W.D.

Wash. June 22, 2023) (dismissing KCPA claim where plaintiffs "simply alleged the elements of the cause of action without sufficient factual support")). Plaintiffs do not dispute that that standard applies, but contend that their allegations meet that heightened standard. Opp. at 29 [Doc No. 38] (citing Complaint ¶¶ 40, 42). Paragraph 40 alleges that "Zoll misrepresented to Plaintiffs . . . via its Privacy Policy that it has implemented measure to protect from theft and misuse Plaintiffs' . . . Private Information," and that on information and belief, "including from information gathered from the Data Breach at issue and subsequent cybersecurity issues within Zoll's computer network, that representation is not true." Compl. ¶ 40 [Doc No. 33]. Paragraph 42 merely recites the contents of ZOLL Medical's letter notifying Plaintiffs of the Data Breach. Id. ¶ 42.

This is insufficient to overcome the heightened standard of Rule 9(b). From these allegations, the only averment that ZOLL Medical actually knew its security measures were inadequate at the time it represented otherwise to Plaintiff Becker is the fact that data breaches later occurred. This is analogous to the "fraud by hindsight" doctrine applied in securities fraud cases. Under that doctrine, "a complaint may not simply contrast a defendant's past optimism with less favorable actual results" to overcome the Rule 9(b) pleading standard. Karth v. Keryx Biopharmaceuticals, Inc., 6 F.4th 123, 135 (1st Cir. 2021) (internal quotation marks and citation omitted). Cf. Griffey v. Magellan Health Inc., 562 F. Supp. 3d 34, 50 (D. Ariz. 2021) ("As a matter of logic, however, the existence of an adequate data security infrastructure and two data breaches in a year are not mutually exclusive.").

Because the Complaint fails to plead with particularity under the Rule 9(b) standard, the court dismisses the KCPA claim.

J. New York Consumer Protection Act

The NY GBL prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state." N.Y. Gen. Bus. Law § 349. A plaintiff bringing a claim under this law "must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice." Koch v. Acker, Merrall & Condit Co., 18 N.Y.3d 940, 941, 967 N.E.2d 675 (2012) (citations omitted).

ZOLL Medical argues Plaintiff Pacholczak's NY GBL claim should be dismissed because he fails to plead: (1) a nexus to New York; (2) a promise to safeguard information so as to constitute a deceptive practice; and (3) requisite damages. The court finds Plaintiff Pacholczak has not pleaded a sufficient nexus to New York.

ZOLL Medical suggests the NY GBL cannot be invoked because application of the law hinges on where the cyberattack took place, which in this case was not New York. Def.'s Mem. at 27 [Doc No. 37]. Plaintiffs claim the NY GBL instead "focuses on the aggrieved." Opp. at 30 [Doc No. 38]. Both are incorrect.

In Goshen v. Mut. Life Ins. Co. of New York, the New York Court of Appeals held that the territorial reach of the NY GBL "does not turn on the residency of the parties. As both the text of the statute and the history suggest, the intent is to protect consumers in their transactions that take place in New York State." 98 N.Y.2d 314, 325, 774 N.E.2d 1190 (2002) (emphasis added). "After Goshen, however, a split among courts developed as to whether a plaintiff must complete the relevant transaction in New York, or whether the victim may plead a claim by showing a sufficient connection between the deceptive conduct and the transaction, 'requir[ing],

for example, that a plaintiff actually view a deceptive statement while in New York . . . .'" Haft v. Haier US Appliance Sols., Inc., 578 F. Supp. 3d 436, 459 (S.D.N.Y. 2022) (quoting Cruz v. FXDirectDealer, LLC, 720 F.3d 115, 122-24 (2d Cir. 2013)).

In the data breach context, courts have found a sufficient nexus to New York where the collection of private information occurred as the result of a transaction with the defendant in New York. See, e.g., In re Marriott, 440 F. Supp. 3d at 493 (plaintiffs alleged they "were deceived in New York" and "transacted with Marriott in New York by making hotel reservations from New York and/or staying in Marriott properties based in New York"); Smallman v. MGM Resorts Int'l, 638 F. Supp. 3d 1175, 1206 (D. Nev. 2022) (plaintiff alleged transaction by "making hotel reservations from New York and paying any necessary room deposits [from] New York"); In re Cap. One, 488 F. Supp. 3d at 424-25 (each plaintiff "applied for and used [his and her] . . . credit card in New York, and provided [his and her] PII to [defendant] in order to do so").

Plaintiff Pacholczak fails to make comparable allegations here. The only allegation suggesting any connection to New York is that he "is a natural person, resident, and citizen of New York." Compl. ¶ 24 [Doc. No. 33]; see also id. ¶ 197 (same). As noted above, residency alone is insufficient. See Goshen, 98 N.Y.2d at 325. And Plaintiff Pacholczak's remaining allegations are merely a recitation of elements for the NY GBL. See Compl. at 82-84 ¶¶ 228-234 [Doc No. 33]. Unlike with the Florida Plaintiffs' FDUTPA claim, Plaintiff Pacholczak does not allege that ZOLL Medical engaged in any activities in New York. Cf. id. at 75 ¶ 202.

These allegations are like those rejected by the court in In re GE/CBPS Data Breach Litig., 2021 WL 3406374, at *13 (S.D.N.Y. Aug. 4, 2021). There, the plaintiff alleged in

conclusory terms that "the confidential information compromised in [the] Data Breach was likely stored and/or maintained in accordance with practices emanating from [New York] . . . but none of his specific allegations regarding [Defendant's] promises to its employees and their beneficiaries regarding protection of PII, the data protection measures Defendants did and did not take, and the manner in which Defendants notified affected persons about the Data Breach identifies the location(s) where Defendants' relevant conduct took place." Id. (emphasis added). The court therefore found the plaintiff had failed to establish "the requisite nexus between specific deceptive conduct and New York." Id. The same is true here.

Because Plaintiff Pacholczak fails to plead sufficient nexus to state a claim under the NY GBL, the court need not reach ZOLL Medical's other arguments about a deceptive act or damages. The claim is dismissed.

K. Illinois Consumer Fraud and Deceptive Business Practices Act

The Illinois Plaintiffs' ICFA claim fails for the same reason. The ICFA states that "[u]nfair methods of competition and unfair or deceptive acts or practices . . . in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby." 815 Ill. Comp. Stat. 505/2. It requires, however that "the disputed transaction occur primarily and substantially in Illinois," Avery v. State Farm Mut. Auto. Ins. Co., 216 Ill. 2d 100, 187, 835 N.E.2d 801 (2005), even if the plaintiff is an Illinois resident. Archey v. Osmose Utilities Servs., Inc., 2022 WL 3543469, at *5 (N.D. Ill. Aug. 18, 2022) (citing Perdue v. Hy-Vee, Inc., 455 F. Supp. 749 (C.D. Ill. 2020)). In the data breach context, courts have dismissed ICFA claims where the plaintiffs failed to allege that the collection of private information occurred in Illinois. See, e.g., Archey, 2022 WL 3543469, at *5 (no ICFA

claim stated where plaintiff failed to allege that the "cyberattack occurred in Illinois or that Osmose stored [Archey]'s information in Illinois" or that "Osmose asked for, or that he provided his personal information to Osmose in Illinois"); see also In re MCG, 2023 WL 3057428, at *7 (no ICFA claim stated against healthcare consulting company where plaintiff alleged he was a patient with "an Indiana University Health Affiliated Covered Entity," but did not allege he "was a patient of an entity located in Illinois" or that defendant "contracted with an entity located in Illinois or that any data breach occurred in Illinois").

As with Plaintiff Pacholczak's NY GBL claim, Illinois Plaintiffs allege no conduct occurring in Illinois and only identify themselves as residents of Illinois. See Compl. ¶¶ 17, 25 [Doc No. 33]. Plaintiffs' opposition claims that "while both [named plaintiffs] were in Illinois, [they] provided their personal information to Zoll to be prescribed Zoll medical devices." Opp. at 33-34 [Doc No. 38]. But the cited paragraphs do not support this assertion; the Complaint does not actually allege that the Illinois Plaintiffs were in Illinois at the time they provided ZOLL Medical with their Private Information, or that they were prescribed these devices in Illinois. See Compl. ¶¶ 96, 213 [Doc No. 33]. Because the sole allegation of Illinois residency is insufficient, see Archey, 2022 WL 3543469, at *5, the Illinois Plaintiffs have failed to allege a sufficient nexus with Illinois so as to state a claim under the ICFA.

The court need not address ZOLL Medical's remaining ICFA arguments. The claim is dismissed.

L. Pennsylvania Unfair Trade Practices and Consumer Protection Law

The UTPCPL prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce as defined by" the statute. 73 Pa. Stat. § 201-

3(a). ZOLL Medical seeks dismissal of the UTPCPL claim for failure to plead two required elements: ascertainable loss and justifiable reliance. See In re Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 514, 541 (M.D. Pa. 2021).

1. Ascertainable Loss

"To allege an ascertainable loss, the plaintiff 'must be able to point to money or property that he would have had but for the defendant's fraudulent actions.'" In re Rutter's, 511 F. Supp. 3d at 541 (citations omitted). "These damages must be identifiable and 'cannot be speculative.'" Id. (citations omitted). In the data breach context, allegations of lost time are insufficient without "allegation[s] that [plaintiffs] lost any money as a result" of that lost time. Id. ZOLL Medical challenges Plaintiff Gerth's allegations as conclusory. Def.'s Mem. at 30 [Doc No. 37] (citing Compl. ¶ 242 [Doc. No. 33]). But Plaintiff Gerth has not asserted a UTPCPL claim, and ZOLL Medical has not challenged the sufficiency of Plaintiff Bendriss's allegations of loss for this claim.

2. Justifiable Reliance

The UTPCPL claim fails to allege justifiable reliance. "To bring a private cause of action under the UTPCPL, a plaintiff must show that he justifiably relied on the defendant's wrongful conduct or representation and that he suffered harm as a result of that reliance." Yocca v. Pittsburgh Steelers Sports, Inc., 578 Pa. 479, 501, 854 A.2d 425 (2004).

Plaintiffs argue that Bendriss alleged reliance on ZOLL Medical's "[m]isrepresent[ations] that it would protect the privacy and confidentiality of [her . . .] Private Information, including by implementing and maintaining reasonable security measures" and "that it would comply with common law and statutory duties pertaining to the security and

privacy of [her] Private Information[.]" Compl. at 85-86 ¶¶ 237(d)-(e), 240 [Doc. No. 33]; Opp. at 33 [Doc. No. 38]. The only specific facts from the Complaint pertaining to such misrepresentations are that ZOLL Medical represented in its privacy policy that it "[has] implemented measures designed to secure [Plaintiffs' and Class Members'] personal information from accidental loss and unauthorized access, use, alteration, and disclosure." Compl. ¶ 40 & n.4 [Doc. No. 33]. As noted above, however, the privacy policy further states that it will "undertake reasonable efforts to protect [Plaintiffs'] personal information" but "cannot guarantee its security." Def.'s Mem. at 23 [Doc No. 37]; Compl. ¶ 40 & n.4 [Doc No. 33] (citing Privacy Policy, ZOLL Med. Corp., https://zoll.com/privacy-policy). Thus, the court finds Plaintiff Bendriss's allegations too conclusory to consider true at this stage. See In re Rutter's, 511 F. Supp. 3d at 542 (finding no justifiable reliance where plaintiffs only "make certain allegations pertaining to [defendant's] privacy policy and that 'Plaintiffs and class members provided their Card Information to [defendant] with the reasonable expectation that [defendant] would comply with its obligations to keep the card information confidential and would secure it from unauthorized access[]'"). As in In re Rutter, Plaintiff Bendriss "fail[s] to explicitly plead [her] reliance on the privacy policy itself[.]" Id. (emphasis in original).

Plaintiffs further argue that justifiable reliance based on an omission can be satisfied by showing "that [Bendriss] would not have purchased a product had [she] been aware of the defect." Miller v. Hyundai Motor Am., 2017 WL 4382339, at *9 (S.D.N.Y. Sept. 29, 2017) (citing Zwiercan v. Gen. Motors Corp., 58 Pa. D. & C.4th 251, 2002 WL 31053838 at *4-5 (Com. Pl. 2002)). However, the two cases cited for this proposition are inapposite because they involved affirmative duties by manufacturers to disclose material safety information. See Miller,

2017 WL 4382339, at *1 (defects in vehicle braking system); Drayton v. Pilgrim's Pride Corp., 2004 WL 765123, at *1 (E.D. Pa. Mar. 31, 2004) (listeria-contaminated meat products).

The court in In re Rutter's addressed and rejected the same line of argument. There, plaintiffs brought a UTPCPL claim based on a data breach incident and argued they had pleaded justifiable reliance because their claim was omission-based in reliance on Drayton (the contaminated-meat case) and Zwiercan (another vehicle safety defect case). See In re Rutter's, 511 F. Supp. 3d at 542. The court found disingenuous the argument that the deceptive conduct was solely based on omissions, as plaintiffs had pleaded their cause of action (albeit in conclusory language) on affirmative conduct such as "representing" and "advertising," in addition to alleged omissions. Id. at 542-43. More importantly, the court found that Zwiercan and Drayton "involved manufacturers of potentially-dangerous products who were ostensibly aware that their products had material defects but did not alert any customers"; the cases were inapplicable in a data breach case where "Plaintiffs were not purchasing any potentially-dangerous products" and the defendant "was not duty-bound . . . to alert customers or state or federal officials as to any potential data-security issues." Id. at 543-44. Finally, the court found that the plaintiffs "fail[ed] to explicitly plead their reliance on the privacy policy itself or any other representations made by Rutter's on the subject." Id. at 542. They only included conclusory allegations of reliance. Id. On the same point, the court noted that the plaintiffs in Zwiercan and Drayton "were totally unable to establish the reliance element—in both cases, 'the unsophisticated Plaintiff is at the mercy of the Defendant to inform her of a known safety defect.'" Id. at 544 (citation omitted). The data breach plaintiffs, by contrast, alleged that the defendant "did make representations as to its continuing efforts to safeguard personal data—

Plaintiffs just cannot establish they actually relied on those representations prior to making purchases." Id.

That analysis is largely applicable here. Plaintiff Bendriss cannot claim she was purchasing potentially dangerous products or that ZOLL Medical was duty-bound to alert customers or government officials to any potential data-security issues. And although the Complaint discusses ZOLL Medical's privacy policy, it does not explicitly allege that Plaintiff Bendriss relied on it prior to deciding to use a ZOLL Medical device. See Compl. ¶ 40 [Doc No. 33]. The other allegations of reliance are conclusory and therefore insufficient. See, e.g., id. at 86 ¶ 240 (Plaintiffs "justifiably relied on the above-mentioned misrepresentations"); id. at 86 ¶ 241 (Plaintiffs "would not have engaged in business with Zoll . . . but for Zoll's misrepresentations").

As such, Plaintiff Bendriss has failed to allege justifiable reliance so as to state a claim under the UTPCPL. The claim is dismissed.

IV. Conclusion

For the foregoing reasons, ZOLL Medical's Motion to Dismiss [Doc. No. 37] is GRANTED as to: standing for allegations of spam and diminution in value of their Private Information; Plaintiff Becker's negligence claim under Kansas law; the breach of implied contract claim as to an implied-in-fact contract; the breach of implied contract claim as an implied-in-law contract only as to Plaintiffs Gerth and Weese; the claim for declaratory and injunctive relief; the Illinois Plaintiffs' ICFA claim; Plaintiff Becker's KCPA claim; Plaintiff

Pacholczak's NY GBL claim; and Plaintiff Bendriss's UTPCPL claim. These claims are dismissed.[19]

ZOLL Medical's Motion to Dismiss [Doc. No. 37] is DENIED as to: standing on all other grounds raised; the negligence claim under Massachusetts, Pennsylvania, Illinois, Florida, Texas, and New York law; the breach of fiduciary duty claim; the unjust enrichment claim; the breach of implied-in-law contract claim as to Plaintiffs Priddy, McGilberry, Jemison, Becker, Bendriss, Brown, Pacholczak, and McMahon; and the Florida Plaintiffs' UTPCPL claim.

IT IS SO ORDERED.

March 31, 2025

/s/ Indira Talwani
United States District Judge

[19] As the court noted above, the negligence per se claim is voluntarily dismissed.